AMENDMENTS TO THE CLAIMS

Claims 1-4 (canceled).

5.   (Currently amended) A method of attestation comprising:

connecting a computer having no operating system installed thereon, and having firmware and a trusted platform module (TPM) coupled to said firmware to a network;

determining a current platform trust state for said computer, wherein said current platform trust state is based on a current state of said firmware;

receiving a challenge from a challenger on said network, wherein said challenger holds an enrolled platform trust state for said computer;

signing said current platform trust state with a private portion of an attestation identity key (AIK);

providing said signed current platform trust state to said challenger; and

accessing said network when said signed current platform trust state matches said enrolled platform trust state.

6.   (Original) The method of claim 5, wherein said TPM comprises a plurality of platform configure registers (PCR) and determining a current platform trust state comprises: performing a hash-extend operation on contents of said PCRs.

7.   (Original) The method of claim 5, further comprising:

provisioning said computer across said network.

8.   (Currently amended) A method of provisioning, comprising:

detecting a new computer having no operating system installed thereon on a network;

challenging said new computer;

receiving a current platform trust state, signed with a private portion of an attestation identity key (AIK), from said new computer;

4

comparing said signed current platform trust state with an enrolled platform trust state, wherein said enrolled platform trust state is signed by a privacy certificate authority; and

allowing said new computer to access said network when said enrolled platform trust state and said signed current platform trust state match.

9.   (Original) The method of claim 8, further comprising:

verifying trust in said privacy certificate authority; and

allowing said new computer to access said network when said privacy certificate authority is trustworthy.

10.   (Currently amended) An apparatus, comprising:

a processor;

firmware, coupled to said processor;

a trusted platform module (TPM), coupled to said firmware;

a plurality of platform configuration registers (PCR) coupled to said TPM, wherein said PCRs contain a first platform state signed by a privacy certificate authority; and

an attestation identity key (AIK), maintained by said TPM, wherein said AIK comprises a public and private key;

wherein the apparatus has no operating system installed thereon;

wherein said TPM is operative to calculate a platform state signed with said private portion of said AIK according to a platform state contained in said PCRs, and is operative to provide said calculated platform state to a challenging network; and

wherein a comparison of said first platform state and said calculated platform state being identical indicates that the apparatus has not been tampered with.

11.   (Original) The apparatus of claim 10, wherein said firmware is at least one of extensible firmware interface (EFI)-based firmware, IEEE 1275 open firmware, LinuxBios, or a PC/AT BIOS.

12.   (Canceled).

13.   (Previously presented) The apparatus of claim 10, wherein said firmware is operative to provide said public key of said AIK and said platform trust state without an operating system running on said processor.

14.   (Currently amended) A machine-accessible medium containing software code that, when read by a computer, causes the computer to perform a method comprising:

        detecting a new computer on a network, said computer having no operating system installed thereon, and having firmware and a trusted platform module (TPM);

        challenging said new computer;

        receiving a current platform trust state signed with a private portion of an attestation identity key (AIK) from said new computer;

        comparing said signed current platform trust state with an enrolled platform trust state, wherein said enrolled platform trust state is signed by a privacy certificate authority; and

        allowing said new computer to access said network when said enrolled platform trust state and said signed current platform trust state match.

15.   (Original) The machine-accessible medium of claim 14, wherein the software code causes the computer to perform the method further comprising:

        verifying trust in said privacy certificate authority;

        preventing said new computer from accessing said network when said privacy certificate authority is not trustworthy; and

        allowing said new computer to access said network when said privacy certificate authority is trustworthy.

16.   (Currently amended) A machine-accessible medium containing software code that, when read by a computer, causes the computer to perform a method comprising:

        determining a current platform trust state for a computer having no operating system installed thereon, and having firmware and a trusted platform module (TPM) coupled to said

firmware, wherein said current platform trust state is based on a current state of said firmware and said computer is coupled to a network;

      receiving a challenge from a challenger on said network, wherein said challenger holds an enrolled platform trust state for said computer;

      signing said current platform trust state with a private portion of an attestation identity key (AIK);

      providing said signed current platform trust state to said challenger; and

      accessing said network when said signed current platform trust state matches said enrolled platform trust state.

17.   (Original) The machine-accessible medium of claim 16, wherein said TPM comprises a plurality of platform configure registers (PCR) and determining a current platform trust state comprises:

      performing a hash-extend operation on contents of said PCRs.

18.   (Canceled).

19.   (Previously presented) The machine-accessible medium of claim 14, wherein said enrolled platform trust state is installed in at least one of extensible firmware interface (EFI)-based firmware, IEEE 1275 open firmware, LinuxBios, or a PC/AT BIOS on said new computer.

20.   (Canceled).

21.   (Canceled).

22.   (Previously presented) The method of claim 5, further comprising, prior to connecting said computer to said network:

      bundling an identification (ID) request for said computer;

      sending said ID request to a privacy certificate authority;

receiving a verified and signed ID from said privacy certificate authority; and

installing said verified and signed ID on said firmware.

23. (Previously presented) The method of claim 22, wherein said verified and signed ID is installed in at least one of extensible firmware interface (EFI)-based firmware, IEEE 1275 open firmware, LinuxBios, or a PC/AT BIOS.

24. (Previously presented) The method of claim 22, wherein bundling an ID request comprises bundling at least one of a new public ID key, an endorsement certificate, a platform certificate, or a conformance certificate into said ID request.

25. (Previously presented) The method of claim 24, wherein said new public ID key is a public portion of an attestation identity key (AIK), said AIK having a public portion and a private portion, wherein said private portion is maintained by said TPM.